(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 June 2002 (20.06.2002)

PCT

(10) International Publication Number
WO 02/49311 A2

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/US01/43927

(22) International Filing Date:
14 November 2001 (14.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/711,999 14 November 2000 (14.11.2000) US

(71) Applicant: **TRITRUST.COM, INC.** [US/US]; 39 Karen Road, Newton, MA 02468 (US).

(72) Inventor: **BERENSON, Richard, W.**; 39 Karen Road, Newton, MA 02468 (US).

(74) Agent: **BARZILAY, Ilan, D.**; Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210 (US).

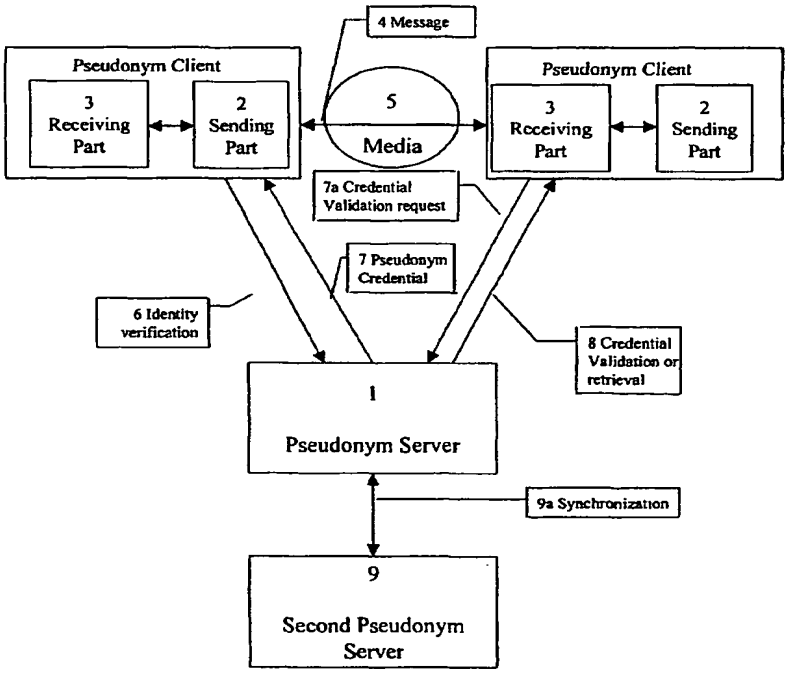
(81) Designated State *(national)*: JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PSEUDONYM CREDENTIALING SYSTEM



(57) Abstract: A Pseudonym Server provides credentials for pseudonyms to clients, which can then use those credentials in interactions with other clients. The credentials are based on proof of right to use a pseudonym, attestations, identity verifications, and/or aggregations. Communication between clients can be over a wide variety of media.

WO 02/49311 A2

PSEUDONYM CREDENTIALING SYSTEM

Field of Invention

The field of this invention is credentialing systems.

Background

Transactions between parties are dependant on one party trusting another and being sure that the "identity" of the other party possesses the characteristics that the first party expects. Many modern interactions occur over a media rather than in person. (For example, fax, phone, and Internet) These mediated interactions pose a problem for identity verification.

The problem of trust is compounded when one party wishes to protect identity (remain anonymous) yet at the same time demonstrate their trustworthiness to a second party. Several systems exist as attempted solutions to this problem, for example the on-line auction house www.ebay.com offers anonymous identification for its users with a feedback service whereby users can rate the trustworthiness of other users. eBay also collects identity information from users but does not share that data between users. Other systems, such as the Thawte Certification gives users a credibility rating which improves with the number of points accumulated.

Systems such as these which are based on pseudonyms are insufficient for transactions which require a more detailed level of identification. (For example credit decisions or voting).

"Digital certificates" issued by a "certificate authority" are used to verify that certain digital files were sent by a particular person. Typically the certificates only verify the electronic point of contact, however may include other identity information of the party owning the certificate. Typically, these other identity characteristics must be proven to the certificate authority before the digital certificate will reflect the particular identity information. These identity characteristics may be certified by a credit bureau or other service such as a public database.

A variety of proposed schemes would allow an individual to present digital credentials without revealing his/her identity. In one, a portable digital assistant or smart card (with internal checks and balances called an "observer" and a "representative") can certify certain facts about an individual. (D. Chaum, T. Pederson, "Wallet Databases with Observers," Advances in Cryptology – CRYPTO '92, pp 89-105 Proceedings,

Springer-Verlag (1993)). This scheme requires that the individual presenting the certificates effectively assert ownership (for example by proving physical possession of it) of the digital assistant, and prove that the digital assistant was not tampered with. This technique is limited when dealing with mediated interactions.

The Dutch Data Protection Authority ("Registratiekamer") has described a system where privilege certificates granted by a service provider would receive a blind digital signature, allowing them to be detached from the pseudonym to which they were assigned. ("Privacy-enhancing Technologies: The Path to Anonymity," Volume II, section 4.1.3. Registratiekamer, The Netherlands, August 1995). The user keeps the assigned privileges and can use them with other service-providers under a different pseudonym.

The role of the third party is merely to collate the certificates into a letter in order to protect the user from revealing his identity to the certificate providers.

Others have described a third party (called an "identity escrow") entrusted with keeping such things as a master key linking digital pseudonyms with the true identities of their users. (Roger Clarke, Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue, Invited Presentation to the Conference on 'Smart Cards: The Issues', Sydney, 18 October 1996). The third party knows that the relationship between a user's true identity and his/her pseudo-identities must be kept completely secret. However, if certain conditions require it (under previously agreed upon terms), the third party is permitted to reveal the user's identity to a service provider.

There are also a variety of known techniques for transferring information about someone without revealing his identity called "Zero Knowledge Proofs."

Another method describes creating digital credentials for pseudonyms that can be transferred between participating organizations without revealing the identity of the pseudonym owner. (Chaum, D. & Evertse, J., "A Secure and Privacy-Protecting Protocol for Transmitting Personal Information between Organizations." Advances in Cryptology – CRYPTO '86, 263 Lecture Notes in Computer Science 118, Springer-Verlag (1987)). This method requires that the pseudonyms and the credentials all be large numbers that are constructed in a particular way.

Summary

None of the above systems offer an effective and believable way to verify characteristics of pseudonyms without revealing an entity's true identity or offer a method for transferring credentials among related pseudonyms.

In one embodiment of the invention a system for verifying characteristics of an entity comprises: one or more modules programmed to: accept proof of a right to use a pseudonym from an entity; create one or more certificates which associates the pseudonym with one or more characteristics of the pseudonym or the entity without associating the pseudonym with the identity of the entity; and send at least one of the one or more certificates to a recipient external to the system.

In another embodiment of the invention a computer readable medium on which is encoded a software program including computer instructions which when executed by a computer cause the computer to execute a sequence of steps comprising: accepting proof of a right to use a pseudonym from an entity; creating one or more certificates which associates the pseudonym with one or more characteristics of the pseudonym of the entity without associating the pseudonym with the identity of the entity; and sending at least one of the one or more certificates to a recipient external to the system.

In another embodiment of the invention a method for verifying characteristics of an entity comprises: accepting proof of a right to use a pseudonym from an entity; creating one or more certificates which associates the pseudonym with one or more characteristics of the pseudonym of the entity without associating the pseudonym with the identity of the entity; and sending at least one of the one or more certificates to a recipient external to the system.

In each of the embodiments of the invention one or more of the following variations may be present:

The invention is executed on part of one or more computer systems. The invention is executed over the Internet. The invention is executed on a portable device. At least one of the one or more characteristics includes a characteristic verifiable by one of the following methods: through physical examination, through prolonged interaction, or by a third party. The invention is capable of receiving characteristic information from an external data source. At least one of the one or more certificates is a digital certificate. The invention is capable of associating a characteristic associated with a first

pseudonym with a second pseudonym. At least one of the one or more certificates includes one or more credentials.

One or more of the following variations may also be present:

One of the one or more credentials included in the one or more certificates is directly or indirectly attributed to the pseudonym. The invention indirectly attributes one or more characteristics to the pseudonym by combining one or more characteristics of the pseudonym or cross-attributing one or more characteristics from other pseudonyms which the same entity has the right to use. The direct attributing is accomplished by an attestation. The attestation is given a reliability weight based on the reliability of an entity providing the attestation. An attestation collection process involves the transfer of an electronic form. At least one of the one or more certificates includes information about the reliability of the source or sources of information contained in the one or more credentials. The invention is capable of detecting a reference loop. At least one of the one or more certificates includes information about when the entity proved its right to use the pseudonym. At least one of the one or more certificates expires within a limited time.

One or more of the following variations may also be present:

The invention is capable of screening outgoing messages to prevent undesired identity or characteristic information from being sent. The invention maintains a voice connection and wherein at least one of the one or more characteristics is a characteristic of an entity at one end of the voice connection. At least one of the one or more certificates contains information certifying the right of the entity to gain access to a restricted group or location. At least one of the one or more certificates contains a ballot and information certifying the right of the entity to vote. At least one of the one or more certificates contains information certifying the right of the entity to send messages to a particular recipient. At least one of the one or more certificates contains information certifying the right of the entity to access restricted data or services. At least one of the one or more certificates contains financial information certifying the right or ability of the entity to engage in one of the following: a financial transaction, an insurance transaction, a medical transaction, an employment transaction, or a consumer transaction.

One or more of the following variations may also be present:

The invention is capable of sending location and movement information of the entity to an authorized entity. Accepting proof of the right to use a pseudonym involves taking a biometric measurement. Accepting proof of the right to use a pseudonym receiving a key obtainable from a third party. Accepting proof of the right to use a pseudonym checking an electrical token. The recipient is the entity. The recipient is a client computer. The proof of the right to use a pseudonym involves a key obtainable from a third party. The proof of the right to use a pseudonym involves an electrical token.

One or more of the following variations may also be present:

The invention includes a client computer executing one of the modules which includes instructions to: send and receive proof of a right to use a pseudonym from an entity; end and receive one or more certificates which associate the pseudonym with one or more characteristics of the pseudonym or the entity without associating the pseudonym with the identity of the entity. The client computer further includes instructions to screen outgoing messages to prevent undesired identity or characteristic information from being sent. The invention includes a server executing one of the modules which includes instructions to: send and receive proof of a right to use a pseudonym; create one or more certificates which associates a pseudonym with one or more characteristics of the pseudonym or entity without associating the pseudonym with the identity of the entity; and send at least one of the one or more certificates to a recipient external to the system. The server further includes instructions to store pseudonym characteristic information. The invention may calculate the reliability of attestors by, for each of a characteristic attestation made: for each on of one or more pseudonym for which the character attestation was made: for each time another entity attested to that characteristic: verify or contradict the attestation; if the attestation is verified, add one to a verification counter (v); if the attestation is contradicted, add one to a contradiction counter (c); if there are no contradictions, add one to the attestation counter (A); if there are contradictions, calculate the raw reliability weight (R_{ACP}) for the attestor for a characteristic of a pseudonym as: $R_{ACP} = v/(v + m*C)$ where m is a reliability coefficient; calculate the raw reliability weight for attestor for a characteristic R_{ACP} as the average of all values of R_{AC} for all pseudonyms; and calculate the raw reliability weight (R_A)as the average (R_{AC}) of for all characteristics.

Brief Description of the Drawings

For a better understanding of the present invention, reference is made to the accompanying drawings in which like reference numerals refer to like objects throughout the figures.

Figure 1 is a block diagram presenting an overview of the operation of the system as a whole;

Figure 2 is a block diagram showing the interaction of elements of the pseudonym server;

Figure 3 is a block diagram illustrating the interaction among the several major sub-processes in the aggregation and validation process;

Figure 4 is a flow chart illustrating the process of calculating pseudonym reliability weights;

Figure 5 is a block diagram showing major elements of the pseudonym client when it is transmitting information about a pseudonym;

Figure 6 is a block diagram showing major elements of the pseudonym client when it is receiving information about a pseudonym;

Figure 7 is a data flow diagram showing an alternative embodiment where the pseudonym client resides in a portable device;

Figure 8 is a data flow diagram showing how an attestation client is used to facilitate attestations.

Detailed Description

To create a practical credentialing system for entities that do not wish to reveal their full identity, it is necessary to understand the nature of identity. Identity characteristics may be split into three categories: (1) those that can be verified quickly, (2) those that can be verified by prolonged interaction, and (3) those that can be verified by third parties.

Verification of a party's identity by making sure the party has sufficient characteristics in common with the identity is typically done with characteristics that are quickly verified through an examination. Examples of these characteristics (referred to here in as category 1 characteristics) include, without limitation; association with a token (such as a passport, dog tag, or barcode), appearance, natural physiography (such as feature measurements, finger prints, or DNA patterns), biodynamics (such as a voice characteristic), social behavior (habits, style of speech), knowledge (such as passwords or mothers maiden name), point of contact (home address or email address).

Category 2 characteristics, these verifiable through prolonged interactions, can be associated once identity is established. Category 2 includes (but is not limited to) characteristics such as reliability, responsiveness, and honesty.

Many characteristics which are necessary to certain transactions can only be verified by third parties. These category 3 characteristics include (but are not limited to) employment status, education, professional license, legal history, credit history, etc.

A third party certification of a characteristic of an identity is called a *credential*. The weight of a credential depends on the trustworthiness of the third party certifying the characteristics.

In certain transactions an entity may wish to verify certain characteristics to another party but may wish to keep other characteristics hidden from the party. Current systems frequently allow one party to view much more than the necessary information about a second party during transactions and may improperly share that information with entities completely unrelated to the transaction. In this manner information may be collected about entities who would rather their information remain private unless necessary.

As names may be shared with multiple entities the unique identifier associated with a single identity is called a "True Name." The United States government issuing Social Security or Employer Identification Numbers is an example of an attempt at creating True Names. Using a True Name in a transaction will automatically verify certain characteristics but prevents a transaction from occurring anonymously. Anonymous transactions may be beneficial in certain situations including (but not limited to) to avoid retaliation, avoid embarrassment, avoid discrimination, and protect

against unidentified risks. A disadvantage to anonymous transaction is that it is impossible to verify certain characteristics or establish a relationship between entities.

Pseudonyms offer a balance between anonymous transactions and those using an entity's True Name. A pseudonym is a label used by an entity to associate certain characteristics with the entity. Pen names, or email addresses are typical examples of pseudonyms.

Currently, only category 2 characteristics can be verified for an entity using a pseudonym in a transaction. This yields two major setbacks. First, it is time consuming and expensive to verify category 2 characteristics. Second, it is difficult to ensure that the entity using the pseudonym is the real owner of the entity and not an imposter. Accordingly, trust is very difficult to develop for pseudonym transactions. Furthermore, many pseudonyms are only useful for a particular media subset (such as an eBay I.D.) and are unavailable for use outside that subset, further prohibiting an entity from transferring credentials belonging to an entity from one pseudonym to another.

Inefficiencies exist in prior systems for transferring credentials between pseudonyms. Systems such as the Registratie Kamer system described above depend on cryptography alone and do not prevent an owner of a digital certificate from transferring that digital certificate to someone else, and so on.

A trusted third party ("TTP") is the term used for an independent third party who is trusted by both the user and service provider alike (comparable to a "digital attorney" or "digital notary"). One particular type of TTP is a Certificate Authority ("CA").

Credentialing System

Described below is an information system, for enabling entities to create and maintain pseudonyms that have verifiable characteristics. In one embodiment, the pseudonyms and credentials are used in the context of a computer network, such as the Internet. While the description below may identify the user of the system as an individual, the system may be used to provide pseudonyms for corporations or organizations as well and is not limited only to individuals. The pseudonyms may be used, for example, in conjunction with an e-Mail service, a Chat room, a discussion list, a scheduling or voting system, or an e-commerce system.

The system is also capable of using pseudonym-credentialing services to facilitate the pseudonymous provision of other services. Examples of such contemplated services include, without limitation: credentialed anonymous messaging (such as chat rooms, anonymous on-line communications, voting); credentialed anonymous access (on-line publications, equipment use, private web-sites); anonymous purchases; pseudonymous applications (credit, insurance, jobs); and pseudonymous data collection.

The system encompasses the use of any type of service accessed through a pseudonym where the provision of the service is contingent on receipt of pseudonym server produced certificates regarding the characteristics of the pseudonym.

An entity may register its True Name and Pseudonym(s) with a Trusted Third Party Registrar (TTPR). The TTPR then collects information associated with the Pseudonym or True Name in order to validate characteristics the individual wishes to be associated with that Pseudonym or True Name. Later, the entity may request and receive from the TTPR a certificate verifying that one or more credentials are associated with a registered Pseudonym; the certificate is based on the characteristics known to be true of the Pseudonym or its True Name. The credential may be stated in such a way as not to reveal the True Name. The TTPR may aggregate information by True Name, so that validated characteristics of one pseudonym may be certified as true of another belonging to the same entity. One TTPR may communicate with another TTPR offering pseudonym credentialing services to determine whether they both are providing pseudonyms for the same True Name. The credential may state how the characteristics have been validated, and whether the registrar checked the other pseudonyms for the same True Name for consistency.

In one embodiment, only an entity that can prove its identity may receive a certification related to a pseudonym. Identity proof can be by presenting a certificate containing data that proves the sender has a sufficient number of Category 3, Category 2, and/or Category 1 characteristics. The amount and nature of the proof requested could be set by the individual and could be reported as part of the pseudonym certificate, if so desired. Certificates may be set to expire relatively quickly, to prevent their being misappropriated.

In another embodiment, the TTPR may request proof of an entity's right to use a pseudonym and provide the entity with a (possibly time-limited) certificate of having

received that proof. The entity then provides the pseudonym-ownership certificate, possibly along with pseudonym credential certificates, to another party as proof that the owner of the pseudonym has the characteristics of the entity.

The TTPR tracks what credentials have been certified for each pseudonym. The entity may also maintain a separate record of what credentials have been certified, and may augment that separate record with a list of claims, true or untrue, which the entity has made about the pseudoidentity of the pseudonym. The entity's private information store may support a service which screens communications made in the name of a pseudonym to ensure information is not revealed about the entity which is inconsistent with or secret for the pseudonym (such as True Name or address). It could also cross-check the claimed characteristics of each pseudonym to suggest how easy it would be for a third party to infer that certain pseudonyms are, in fact, owned by the same True Name.

The TTPR may validate characteristics in a number of ways, among them through documentary evidence, personal references, or an analysis of the consistency of the True Name's claimed characteristics. Documentary evidence such as information from credit bureaus, government agencies, and other sources can be collected and verified. References or information can be collected from other entities or pseudonyms supporting claims by a pseudonym that it has certain characteristics. References may be structured so that the claimed characteristics may be easily extracted from them. References may be aggregated, so that credentials could be issued such as "162 positive references," "80% positive references," and so on. These references may be weighed based on certificates of characteristics about the referring pseudonyms. For example, the reliability weight of references may be calculated by examining the history of references given by the referee.

Certificates about the referrers may be obtained from any TTPR that maintains a pseudonym credentialing service. TTPRs may share True Names to determine whether a reference is from the same person and whether reference-rings have been formed. (A reference ring occurs when a group of entities provide references for each other so that no entity has a reference outside of the ring).

Certain individuals with high trust levels ("notaries") may certify facts or the identity of an individual. The trust level of an individual may be determined by looking at the veracity of facts he or she has certified. Veracity of a fact may be determined by

looking at the number of trustworthy sources that have certified it. There are also a broad set of known artificial intelligence and/or fuzzy logic techniques which have been used to critique credit and other applications. These could be applied to the fact database about any entity. The certification of the TTPR may be used to assure payment for or right to use certain services that could be provided to the pseudonym, including financial services (debit and credit cards, escrow), internet services (including e-mail forwarding, blind IP addresses, etc.), information services, issuing of identification cards, and so on. It may also be used to validate the source of a communication or transaction.

Another application of a credential would be to grant the owner of a pseudonym access to copyrighted material. In one embodiment, the material would be stored on a central server. In another, the material would be stored on a variety of individually owned and maintained computers. The pseudonym owner would present a credential to the server in order to gain access to the materials. The credential would attest to the pseudonym owner's right to obtain a copy of the materials that met specific criteria.

In one embodiment, credentials may be created using cryptographic techniques, such as encryption and digital signatures including, without limitation, X.509 (a known format) digital certificates. In other embodiments, credentials can be printed, looked-up through an information system such as web page possibly based on a pass-code which may or may not be unique to the credential, or imbedded in a token. Credentials may also be created by passing a document through a secure pipe, or any other process which validates that it was sent by the TTP.

System Overview

The illustration below is in the common server/client model. However, this illustration is not meant to be limiting. The system may be entirely located on one computer system or may be implemented such that multiple computers can function as "servers." The server/client implementation is easier to understand and therefore discussion of this implementation is not meant to limit the structure of the system.

Figure 1 shows the major elements of the system and how they interact. The Pseudonym Server (1) may be operated by a Trusted Third Party Registrar (TTPR), which may be (among other things) a law firm, escrow agent, financial institution, Internet service provider, or trusted computer system. In the preferred embodiment, the

Pseudonym Server (1) is a computer system that includes a database and a processor. In another embodiment, the Pseudonym Server can be a distributed or peer-to-peer architecture system. Alternatively, there may be several Pseudonym Servers, possibly operated by different TTPRs, which are simultaneously in contact with the Pseudonym Client. The Pseudonym Server need not be in a single physical location or controlled by a single entity.

A Pseudonym Client may be split into two major elements: a sending part (2) and a receiving part (3). While each user has access to both elements, interaction is between complementary elements being accessed by two different users. The sending element of a Pseudonym Client (2) transmits one or more messages (4) through one or more media (5) to the receiving element of a Pseudonym Client (3). In one embodiment the sending port (2) and the receiving port (3) are located on the same computer device.

In a preferred embodiment, the Pseudonym Client is a software module that is attached to and/or works with other software that runs on a user's local computer. However, the Pseudonym Client may also be a stand-alone application that runs on the user's local computer or a server-based application or module that the user accesses over a network. For example, the Pseudonym Client may be accessed through a web page. The Pseudonym Client may also be an integral part of a device, such as a smart card, dongle, electronic key, PDA, or other portable or handheld computing device. The Pseudonym Client could also be part of a "trusted console" (a computer system where the ability to spoof the presence of a user has been limited).

The Pseudonym Server (1) may interact with a Pseudonym Client (2 & 3) in (without limitation) several ways: the server can request and receive identity verification from the sending element of a Client (6), it can send credentials to the sending element of a Client (7), it can receive a request for credential validation (7a), and it can send credentials to or validate claimed credentials for a receiving element of a Client (8).

The Pseudonym Server (1) can interact with a Second Pseudonym Server (9) in a process called Synchronization (9a), in which the two servers determine if they have any True Names in common. One purpose of Synchronization is to be able to detect possible abuses. One such abuse is when someone gives himself a good reference using a pseudonym. Such an implementation is but one example of how the system is capable of having multiple points of trust implemented through a distributed peer-to-peer

implementation of the Pseudonym Server. Another example would be the use of two or more Pseudonym Servers in a check-and-balance system to assure the trustworthiness of each such server.

Pseudonym Server

A Pseudonym Credential Server (1) produces credentials. Figure 2 describes the inner workings of one embodiment of this aspect of the system. The Pseudonym Ownership Certificate Server (10) is a part of the Pseudonym Server that performs identity verification (6) with the Pseudonym Client (2). It checks the information received from the Client against what is in the Pseudonym Characteristics Database (13) and, if the match meets preset criteria, issues a certificate to the client that the client is currently being accessed by someone who meets the preset criteria. In one embodiment, the issued certificate may expire within a short time period to reduce the likelihood that the certificate might be co-opted by an unauthorized user. If the period is sufficiently short, the TTPR may issue more than one such certificate during the course of an interaction between two Pseudonym Clients.

The Pseudonym Certificate Server (11) issues certificates attesting to the connection between a pseudonym and certain characteristics. The Certificate Server (11) is a part of the Pseudonym Server(1) that responds to a request from a Pseudonym Client by providing credentials to a sending client (2) or to a receiving client (3). Before issuing a certificate, the Pseudonym Certificate Server checks with the Pseudonym Characteristics Database (13) to determine if the requested credential, or one substantially similar to it, can be issued. In one embodiment, certificates may have been both authorized to be sent by the pseudonym owner to the requester and have a factual basis, as attested to in the Pseudonym Characteristics Database (13).

The Verification Interface (12) interacts with a receiving pseudonym client (3) to verify whether a previously issued credential is still valid (i.e., has not been revoked or expired), is still true, and/or needs to be modified/updated. In doing so, the verification interface interacts with the Pseudonym Characteristics Database (13).

The Pseudonym Characteristics Database (13) contains information on the verified or attributed characteristics of each pseudonym. Characteristics may be directly attributed to a pseudonym (e.g., by an attestation service (16) or, if the pseudonym is a

True Name, by a Verification Service (17)), or indirectly attributed by an aggregation and validation process (14).

Characteristics attributed to one pseudonym may be cross-attributed to another, related (i.e. sharing the same True Name) pseudonym by the Aggregation & Validation Process (14). This process can utilize a separate PseudoID to TrueID Map (15) in making these further attributions. Characteristics can be recorded in the Characteristics Database in several ways, including but not limited to those shown in Figure 2. Certifiable characteristics (18) can be entered into the database by an Attestation Collection Service (16), which determines the weights assigned to the characteristic-pseudonym connection based, in part, on the reliability weights (19) stored in the Database as being associated with the source of the attestation. The Certifiable Characteristics (18) can also be recorded by an ID Verification Service (17), which verifies characteristics associated with a True Name by checking external databases (20), such as government, credit, or consumer databases.

The Pseudonym Characteristics Database (13) may list characteristics and their values for each pseudonym in a Certifiable Characteristics Table. In one embodiment, a pseudonym is represented by a unique PseudoID number. Characteristics that can be represented in the table include, by way of example and without limitation: whether the PseudoID is a TrueID (i.e. a PseudoID for a True Name), the Nym (human-language name) associated with the pseudonym, the reliability of attestations made by the pseudonym, the characteristics of the entity behind the pseudonym.

Associated with each such characteristics-record may be, without limitation, a data structure representing the value of that characteristic, a date when the record was created or modified, comments (where, for example, free-text references can be recorded), a source type (for example, whether the record came from an attestation service (16), an ID verification service (17), some kind of aggregation process (14), or another, related pseudonym), the pseudonym of the specific source of the information, the weight associated with the attestation, and whether or not there are restrictions on to whom credentials about this characteristic can be issued (such restrictions are enumerated in a separate table).

Not all records need to be accessed in determining whether to issue a certificate. For example, if an aggregation process has created an aggregation-type record, only that record is normally accessed if a certificate of that characteristic were requested.

Individual issued certificates may be listed in an entry in a Certificate Issuance Journal Table, also stored in the Pseudonym Database (13). This table is particularly important with respect to Pseudonym Ownership Certificates, since it enables the analysis of where the Pseudonym Owner is physically located at different times in order to detect potential identity fraud.

Figure 3 shows the interaction of major sub-processes of the Aggregation and Validation Process (14). Part of this process is (23), in which additional Certifiable Characteristics records for a pseudonym are added to the table in the database (13) based on the existence of such records for different pseudonyms that have the same True Name with first pseudonym, according to the PseudoID to TrueID Map (15). It is within the scope of this invention to allow some or all of the characteristics of a pseudonym to be propagated to other related pseudonyms by the Characteristic Propagation process (23), although, in one embodiment, which characteristics are propagated may be regulated by the pseudonym owner.

Typically, after this process has run, three additional sub-processes may run. The first (24) interacts with other pseudonym servers to detect reference loops. One example of a reference loop is where one pseudonym attests to a characteristic of another pseudonym that has the same True Name as the first. This can be easily detected through a lookup in the PseudoID to TrueID database (15). However, because an individual can register pseudonyms with multiple pseudonym servers, it is useful to check with other servers to ensure there are no reference loops. There are known protocols for accomplishing this check. A more complex type of reference loop is one where two or more different individuals give reliability references to each other. This type of loop can also be detected using equivalent protocols. If a reference loop is detected for a True Name, it is recorded in the Pseudonym Characteristics Database. The reliability calculation (25) uses the existence of reference loops to reduce the reliability score of an attestor.

The second sub-process (25) analyzes the database to determine the reliability of attestors. In a preferred embodiment, this sub-process reflects the assumption that testers

whose attestations are confirmed by other attestors are considered more reliable; those which are contradicted by others are considered less reliable. Figure 6 describes this sub-process in more detail.

Figure 4 describes one embodiment of the reliability weight calculation. Raw reliability weights can have at least two flavors: overall attestor reliability weights (28) and characteristic-specific attestor reliability weights (27). Raw weights can be adjusted (29) based on the presence of any reference loops for the attestor, on the number of sole source references (a large value of "A" could, for example, lessen the reliability weight), for reliability references given by other, reliable attestors, or based on other, certifiable characteristics of the pseudonym which give the individual credibility (such as official titles, professional qualifications, membership in certain organizations, and so on).

The third sub-process (26) calculates aggregate and reconciles characteristics from individual attestations in the Pseudonym Characteristics Database (13) and creates or updates corresponding records in that database. These aggregate characteristics may be based on mathematical calculations (e.g., number or percentage of positive references), or logical inferences (e.g., the person is eight years old, therefore they have no children) or on any other sort of algorithm. For example, the third sub-process (26) of the aggregation and validation process can be implemented through a rule-based system.

It is within the scope of this system to have the various sub-processes of the aggregation & validation process run, without limitation, sequentially, in parallel, iteratively, in a deeply integrated way, in real time, and/or in batch mode.

One embodiment of a protocol that may be used in gathering attestations starts with someone, a pseudonym owner or a third party, sending to the TTPR a request for an attestation. In one embodiment, the initiation request includes information about the characteristic that is to be attested to. The TTPR then sends a request for verification to either the initiator or to a second party attestor who can attest to the pseudonym's association with the characteristic. The attestor verifies the characteristic and returns the verification to the TTPR. In one embodiment, this verification may be through an interactive questionnaire transmitted over the Internet. In another embodiment, the verification is returned along with certifications as to the characteristics of the attestor, preferably using the mechanisms of this system. In another embodiment, verification

can include text comments of the attestor. Verifications can serve as feedback-references on specific transactions, or general character references.

In one embodiment, the stations gathering may take place over an electronic communications network, such as the Internet, including, without limitation, via World Wide Web, email, or instant messaging protocols. The request for attestation may be an interactive electronic form that the requesting party fills out and transmits to the TTPR. The request for verification may be in the form of an interactive electronic form that the attestor completes and returns to the TTPR.

Once verification is received by the TTPR, the comment field associated therewith is scrubbed to remove any names or pronouns that might reveal the True Name of the attestor or of the attestee. Reliability weight information (19) is then retrieved from the Pseudonym Characteristics Database (13) and attached to the verification information. The verification information is then stored in the database (13) as a certifiable characteristics record (18).

In an ownership proof protocol the TTPR and the pseudonym owner first agree to the level of proof that will be required to prove identity. The required proof can involve demonstrating any type or combination of Category 1 characteristics. For example, it can require, without limitation, reciting a password, showing possession of a physical or software token, delivering current biometric data, or giving proof of one's physical presence at a workstation. The level of proof agreed upon depends, in part, on the assessment by the pseudonym owner of the risks that he, she or it might be impersonated.

Once the level of proof required has been set, identity proof and certification sessions can take place, preferably secured by encryption protocols. One example of such a protocol is SSL. In one embodiment, the pseudonym ownership certificate provided by the TTPR to the pseudonym owner has a relatively near term expiration date (in a preferred embodiment, anywhere from one second to one day, depending on the security risks and requirements). In a complementary embodiment, the certificate provided includes information about the level of proof that was presented in proving pseudonym ownership.

There are occasions when more than one individual may have the right to use a pseudonym. For example, the pseudonym could belong to an organization. In such a case, once the individual has proven his identity, the Pseudonym Ownership Certificate

Server (10) checks the Pseudonym Characteristic Database (13) to see if that individual has the right to use the pseudonym; if they do, a pseudonym identity certificate is issued to that individual. The individual could then receive and credibly use certificates belonging to that group, such as a certificate of the right to access certain information.

Another part of the ownership proof process is post facto reviews of the certificates that have been issued in order to detect patterns that may indicate impersonation fraud. For example, if certificates were requested by an individual from two different locations at proximate times, the review could raise an alarm or report some doubt in future certificate releases.

It is within the scope of this system that certificates be signed and date-stamped, for example using X.509 digital certificates issued by a credible certificate authority. In one embodiment, certificates can contain caveats about the characteristics certified, including but not limited to for how long the certification is good for, whether this certification has been checked against the TrueID, how the characteristic was verified, whether there are written reference to back it up, and whether the certificate was issued to the normal physical or logical locus of the Pseudonym owner.

The credentials issued may be short lived (i.e., set to expire within a few seconds to a few days from when they are issued). Using such short-lived certificates are practical with this system because, in many applications, they are used within the context of a defined and certified session. Using such short-lived certificates is useful because it helps reduce the risk that someone has "stepped-in" to assume the identity of the pseudonym owner, and because it eliminates the need for such devices as a certificate revocation list or the online certificate status protocol.

The certificates can also be paper certificates where the system is able to print and mail (via the Postal service or similar carrier) a certificate.

Pseudonym Client

Figure 5 shows the inner workings of a preferred embodiment of a sending Pseudonym Client (2). This version of the client has several functions: it acquires certificates, helps the pseudonym owner organize them, and transmits them to others in association with messages. In one embodiment, the client works as follows:

Upon the request of the Certificate Acquirer (40), the Identify Verifier (39) interacts with the user (45) and the Pseudonym Ownership Certificate Server (10) to

obtain a pseudonym ownership certificate. The interaction with the server (10) preferably follows the ownership proof protocol described above. The interaction with the user (45) may be direct or indirect. For example, it can require that the user be operating the console of the client computer, or allow the user to be interacting through a remote connection. The interaction typically requires the user or automatic system to provide some information on one or more Category 1 characteristics. The protocol that the Identity Verifier uses to interact with the user depends on the level of confidence and security that the pseudonym has contracted for with the pseudonym server.

The certificate acquirer's (40) main job is to obtain from the server (10), for the certificate repository (41), up-to-date certificates as requested by the Pseudonym Characteristics Manager (42). The Manager's (42) role is to maintain the Pseudonym Characteristics database (43), and to inform the Certificate Acquirer (40) when a certificate should be obtained or updated. The Manager (42) has a direct or indirect user interface through which the user (45) is able to set the characteristics of each pseudonym. The user may not want all characteristics to be certified. This may be because certification is expensive, because they are trying to create a certain persona, because they are seeking a degree of anonymity, or for some other reason.

While the Characteristics Manager (42) may have a direct interface with the user (45), it more typically works though an Interaction Manager (44), which unifies the whole user interface to the client. The Interaction Manager (44) can be, without limitation, a stand-alone client or other application, a plug-in or other add-on to existing client or other software (such applications or software may include, without limitation, a browser, an email client, an IM client, a groupware client, or an audio or video conferencing client), an application module running on a server, such as an application server for a web site, or as an integral part of the Pseudonym Client.

The Pseudonym Client may be, without limitation, a stand-alone application, a plug-in or other add-on to existing client software (including, without limitation, a browser, an email client, an IM client, or an audio or video conferencing client), or an application module running on a server, such as an application server for a web site, which is, itself, accessed through a remote client, such as a browser. The Pseudonym Client may also be integrated as part of a device, such as a smart card, dongle, PDA, or other portable or handheld computing device. The Pseudonym Client may also be

implemented part of a "trusted console" (a computer system where the ability to spoof the presence of a user has been limited). The Pseudonym Client (2) may be implemented in such a way as to work as part of a User Client under the P3P standard. (The P3P, Platform for Privacy Preferences, standard contemplates an "agent" in a browser automatically determining and transmitting approved personal information to a web site.) This list is meant to be illustrative and not limiting, as there are many additionally ways in which the Pseudonym Client might be implemented.

In one embodiment, the Interaction Manager (44) also presents information to, and receives information from, the Message Screener (46). For example, the user (45) could compose a message using the Interaction Manager (44). The Interaction Manager (44) then passes that message along to the message screener (46). The Screener (46) checks the message for the presence of information inconsistent with the pseudonym, and identifies that information to the Interaction Manager, which presents the information to the user. In checking the proposed message, the Screener accesses rules and algorithms in an integrated or separate Rules Base (47), to determine what kind of information should be searched for, and also accesses the Pseudonym Characteristics database (43) to determine which claims are valid. In a preferred embodiment, the Screener may do a key-word search on the proposed message, although more advanced natural language or audio or video analysis techniques may also be used.

In another embodiment, the Message Screener (46) may also examine the pseudonym credentials to look for "unusual" credentials which, if attached to multiple pseudonyms, might be used by an attacker to deduce the common ownership of the pseudonyms. The Pseudonym Server (1) may also perform this credential screening.

Once a message has passed the Screener, it is sent to the Message Packager (48), which combines the message with one or more of: (a) appropriate certificates from the Certificate Repository (41), (b) other claimed characteristics information, and, in one embodiment, (c) any cookies or other user-identification information previously given to the client by a remote server and stored/organized by the Cookie Manager (49). The Packager may also disguise or distort an audio or video information contained in the message to make it harder to identify the sender based on the message. The Packager then passes the enhanced message along to the Standard Communications protocol stack

(50) for the chosen Media. It is contemplated that this system can be used with a broad variety of media.

Another part of the Pseudonym Client is the Pseudonym Selector function. This is a sub-feature of the Pseudonym Characteristics Manager (42) and it sets the "Active Pseudonym," the pseudonym under which the Pseudonym Client is operating at any point in time. The Active Pseudonym affects the behavior of the Message Screener (46).

The Identity Verifier (39), the Interaction Manager (44) or Pseudonym Characteristics Manager (42) may interact with the user through a number of possible devices, including without limitation a keyboard, a token reader, a biometrics input device, or an audio or video input device. This device interacts with the Identify Verifier and with the Pseudonym Selector.

The device has information that proves the bearer is the owner of a particular pseudonym – but does not necessarily prove their identity in general. The device may be a smart-card like device that has a secret (large) number that is uniquely associated with the pseudonym. It may also contain information that can confirm that knowledge held by the bearer is knowledge held by the pseudonym owner. It may do this by analyzing a pass phrase or a biodynamic input from the keyboard. It may also do this by passing out a public key, having the computer encrypt the input, then comparing the result to a value stored in the token. There are a variety of ways. The token may also have a built-in biometric measurement ability (e.g., thumbprint) that it would check against a value stored inside it and only say "ok" to the computer if the value matched.

The Pseudonym Client may be simple in some cases – only identifying the user as the pseudonym owner for purposes of logging-in to a larger system. In this case, all information identifying the pseudonym owner would be passed to the Pseudonym Server; a single "the owner is in" certificate would be passed back and used to log into the larger system. This would enable pseudonymous logging-into entertainment media or remote systems through relatively simple client hardware (game consoles, set-top boxes, internet appliances, PDAs, etc.).

Figure 6 shows the receiving end of one embodiment of the Pseudonym Client (3). A message is received from the media (50) by the Message Parser (54), which sends any cookies or similar server information to the Cookie Manager (49), sends certified and non-certified characteristics information to the Foreign Pseudonym Characteristics

database (53), sends session information to the Pseudonym Characteristics Analyst (51), and passes the message itself on to the Interaction Manager (44).

In the preferred embodiment, Analyst (51) looks at each incoming message and the characteristics of its associated pseudonym using the algorithms and rules in the Rules Base (52) to determine, among other things: whether the proof of pseudonym ownership is sufficient, whether any of the certificates should to be verified, and/or whether the characteristics provided are internally consistent (e.g., age and birth date). Based on this analysis, the Analyst (51) may, among other things: send an inconsistency alert to the Interaction Manager (44); ask the Certificate Retriever and/or Verifier (56) to either retrieve missing certificates about the pseudonym which sent the message from, or to verify certificates which were sent by the pseudonym with, the pseudonym server; and/or update the Foreign Pseudonym Characteristics database based on the results of the analysis.

The Interaction Manager (44), upon receiving information about the message or the sending pseudonym, may, among other things: present the information from the Analyst, along with information from the Characteristics Database, to the user or automatic system (45) which is the Interaction Manager's supervisor for input and/or instructions; and/or send a request for clarification (57) back to the sending pseudonym through the media.

In an alternative embodiment the Pseudonym Client may contain a software module that interacts with other software, which may be on the Pseudonym owner's computer or on some other computer to which the Pseudonym owner's computer is connected.

A specific embodiment of such an interaction which may be used to regulate access to specific files or applications. In the specific embodiment to access an encrypted or otherwise protected file, data record, or software application, the pseudonym owner first obtains a key from a trusted third party register (TTPR). This key is released to pseudonyms which have credentials authorizing access to it. In one embodiment, the key may be accessed within a limited time window and may be destroyed by the TTPR after that time window has passed. In one embodiment, the TTPR that holds the key is not the same as the TTPR that certifies the right to gain access to the key. Once the Pseudonym Client has obtained the key, the client passes the

key on through the Software Interface to the Other Software. In one embodiment, the Pseudonym Client does not permanently store the key so that access may be reauthorized by the TTPR each time access is sought.

One application of this embodiment is to protect data files or records on a computer. The files are encrypted by a special application that gets the encryption key from the TTPR, then destroys any local copies of it. Access rights to these files or records can thereafter be granted pseudonymously, but still denied to unauthorized individuals. For example, an email message might be so encrypted; access to it might be only available to individuals whose Pseudonyms are associated with a specific access credential and only during a specific time window.

In another embodiment, the software that regulates access resides on a server computer. The Pseudonym Client passes the encrypted message or file to the server, along with either the key or with a credential authorizing access to the key for the message. The server then, if necessary, obtains the key using the credential, decrypts the message, and transmits or displays the message to the Pseudonym Client.

In one embodiment of the Pseudonym Client, the client may be portable, residing in a token, such as a device the size of a PDA, of a key-ring fob, or possibly even smaller. Figure 7 illustrates the operation of an example of such an embodiment. The Token Device (92) is possessed by the Pseudonym Owner and may, in some embodiments, be able to accept input (93) from the owner (although in other embodiments, possession of the token is considered sufficient proof of identity). The Token Device (92) itself may have several components, including optionally a processor, memory, a device for producing true random numbers, input devices such as without limitation buttons or other switches, a stylus/touch screen, or biometric input devices, and output devices, such as lights or displays. The Token Device (92) is preferably sealed to prevent tampering. The Token Device (92) contains a Pseudonym Client is capable of interfacing with other equipment. These interfaces may include, without limitation, a physical connection such as a USB connection, a serial or parallel port connection, a mouse or keyboard port connection, a firewire connection, or a smart-card reader connection, or a RF (radio frequency), infrared, or light-based connection.

In one embodiment, a pseudonym is established through the device as follows: either through the Token Device's input device, or through an external client such as the

Attestation Client (89), the Pseudonym Owner indicates to the device that it wishes to establish a new pseudonym. The Pseudonym Owner, optionally, inputs a code or biometric data to the Token Device that the Token Device (92) will then associate with the Pseudonym. The Token Device then generates a private key-public key pair using an appropriate algorithm, and transmits (95) the public key to the Attestation Client (89) to which the Token Device is connected. The Pseudonym Owner then, optionally, enters identifying and other information into the Attestation Client (89) which may be, optionally, attested to by a third party also using the Attestation Client (89).

The Attestation Client (89) then packages this information and passes it on the TTPR, which registers the pseudonym and associated information. In alternative embodiments, the pseudonym's PseudoID may be the public key generated by the Token Device, an ID number generated by the Attestation Client (89), or an ID number generated by the TTPR. In one embodiment, the TTPR may then pass-back information to the Attestation Client (89) which, in turn, passes that information to be stored on the Token Device (92).

At the same or a later time, the Pseudonym User may connect the Token Device (92) to a Device Client (96) (which may be connected to or the same as the Attestation Client). The Device Client (96) may be a computer of any kind, located for example, in a television set-top box, a security system, or a vehicle. After providing proper Input (93) to the Token Device (92), the Token Device (92) is ready to prove the owner is present (97) This is preferably done through a challenge. The Token Device receives a challenge from the TTPR through the Device Client (96). In one embodiment, this challenge is in the form of a secret that has been encrypted using the public key associated with the pseudonym. In this embodiment, the Token Device replies by passing the unencrypted secret back to the TTPR through the Device Client (96), thus establishing the presence of the Pseudonym Owner at the Device Client (96). The TTPR may then pass any requested credentials to the Pseudonym Client on the Token Device (92) through the Device Client (96). Alternatively, the Pseudonym Client may pass stored credentials to the Device Client (96), which may, in turn, forward the credentials to a third party, display them, or use them to make some decision, such as whether to grant physical or information access to some capability.

Credentials passed to the Token Device (92) may be short lived – giving temporary access to some resource for which the credential is required. Such a credential might, for example, be used to allow an individual anonymous access to an entertainment event for which proof of age is required. Another example might be a credential of the results of a medical test – such as of being free of infectious diseases – which might be required before the holder of the Token Device (92) were given access to a sterile zone. There are a variety of other obvious circumstances in which an individual might want to present the results of recent medical tests or other credentials without revealing their identity and to which the system might be applied.

Message and Media

Message structure may vary depending on its use and the particular system embodiment. Messages transmitted using this system preferably contain some pseudonym information. In a preferred embodiment, this information is associated with a message header. It is within the capability of this system for the message as a whole or any part thereof to be represented in natural language text, in semantically tagged text such as XML, as a relational or other database entry, or using any other encoding scheme.

Pseudonym information includes, at minimum, the PseudoID of the pseudonym. It may also include a nym, certified credentials or other claimed characteristics of the pseudonym. A credential itself can be a complex data object. The pseudonym information may be directly included in a message, or indirectly included by reference to a continuous and preferably secure session consisting of two or more messages from the same pseudonym (a "mononym session") in which the information is directly included in another message.

A secure mononym session creates a secure pipe or envelope for communications between two parties that assures a receiving party that the communication is coming from someone with certain characteristics. This envelope can enclose individual messages, or whole communications sessions. It can be implemented, without limitation, through tags placed at a one or more layers in the communications protocol stack (time-based enclosure), through encryption techniques (encryption-based enclosure), or through some combination of the two.

Secure mononym sessions may be operated in several ways. The following examples are not meant to be limiting. One embodiment of implementing a secure session involves a pipe established through the use of public keys. After the Pseudonym Owner has proven their ownership of the pseudonym, the Owner then provides the TTPR with a public key that the TTPR then certifies to the message recipient belongs to the Owner at a particular point in time. The recipient may then use the public key to establish an SSL or other form of secure session with the Owner confident that the session is, in fact, being established with Owner and not a spoofer. This session can be established over an IP masking network. Alternatively, the recipient may receive emails (possibly passed through an email forwarder) digitally signed by Owner using the private key corresponding to the public key and have confidence that the signature belongs to the Owner of the pseudonym rather than someone pretending to be the Owner.

A variant embodiment for implementing a secure session involves a secure pipe established using a single, shared certified session key. After the Owner establishes its identity through a secure session with the TTPR, either the TTPR or the Owner propose a unique session key, to which the other agrees. The TTPR then passes this key on to the recipient, possibly through a secure session. Owner and recipient then establish a secure session between themselves (possibly over an IP masking network). This session may be established using SSL or some other protocol, possibly using the certified session key to establish the secure link. If the certified session key is not being used to encrypt the session the session can be certified by the parties' exchanging information encrypted using the certified session key.

A slightly different approach involves the pipe being maintained by the TTPR, which acts as certifier of the session. After establishing a secure session, which is maintained throughout the interaction, the Owner proves ownership of the Pseudonym to the TTPR. The Owner then passes a message on to the TTPR, which, in turn, certifies to the recipient that the message came from Owner. This method has several advantages, including that the TTPR may provide integrated IP masking/email forwarding services (which might otherwise be obtained separately by Owner), and that the Owner does not risk recipient's sharing session keys with others who might then spoof recipient.

The asymmetric pseudonymity assurance of any of these approaches can be made symmetric by having the recipient also play the role of the Owner and vice versa.

As has been stated, the system is capable of transmitting messages through a wide variety of electronic or other media. The media may be simple (involving a simple routing of a message) or compound (involving some transformation of a message).

Messages sent through a complex media may be routed through one or more proxy servers, such as those taught in U.S. Patent Numbers 5,812,670 or 5,754,938, or an anonymous remailer, in order to protect the anonymity of the source. They can also be sent via a pseudonym intermediary. Such an intermediary could maintain a local database of pseudonym characteristics and certificates in order to facilitate pseudonymous interactions. Such an intermediary can accept and send messages through its own pseudonym clients. At the core of such an intermediary can be an interaction server that manages, tracks, and/or provides services to support the interactions between the communicating parties.

In another embodiment, the complex media may include an intermediate client-side computer system. For example, a Pseudonym Client imbedded in a token might plug into a computing device that would, in turn, establish a connection via physical, wireless, or other connection, to the Pseudonym Server.

In another embodiment, where users use standard clients, such as but not limited to browsers to interact with a central server, an intermediary pseudonym server provides all the pseudonym client capabilities and can even incorporate the functionality of the Pseudonym Server (1). In this embodiment, pseudonym clients and the pseudonym server run on a cluster of one or more computers that are connected by a network.

Identity Set-up

Before this system, the only way to accumulate information about the characteristics of an individual was by associating them with the individual's True Name. Thus, to build a database of characteristics about an individual that the individual can then associate with pseudonyms, the TTPR needs to first establish a reliable association between a True Name and an electronic form of identification. This will generally involve an attestation by a reliable second individual. Methods for verifying the reliability of attestations by that second individual have already been discussed above.

Figure 8 describes an Attestation Client (89) system designed to facilitate attestations. Such a system may be used at the time a Pseudonym Owner begins using the pseudonym credentialing system to provide a base association between characteristics of the Owner and the Owner's method of identifying themselves as the Owner. The Pseudonym Owner appears before the Attestor (88) in a place where they both have access to the Attestation Client (89). In a preferred embodiment, the Attestation Client (89) is running on a local computer, although it is possible to have the Attestation Client (89) running on a remote computer that is accessed through a local terminal or other device. The Attestor (88) presents proof of identity to the client (90d), then, typically after observing (90a) and receiving documentary and other information (90b) from the Pseudonym Owner, conveys information to the Attestation Client (89) (e.g., by typing or filling out a form) as the characteristics of the Pseudonym Owner (90c). The Pseudonym Owner also enters the information he will use to identify himself through a Pseudonym Client as the owner of the Pseudonym (90e). This information may be any Category 1 characteristic, such as a used-password combination, possession of an electronic token, or biometric information. The biometric information may be entered into the computer through some device which communicates directly with the Attestation Client (89) through an electronic or other connection. The order in which elements (90a) to (90e) are performed is not important. After the Attestor (88) indicates that no more of the elements (90a) to (90e) need to be performed, in one embodiment the Attestation Client (89) will perform some consistency checks and ask that additional information be entered. In any case, once any consistency checks are complete, the attestation (92) is passed-on to the TTPR in some electronic or other format.

In one embodiment, the Attestations are transmitted as they are completed. In another embodiment, the attestations are collected and later transmitted to the TTPR in a batch. In a third embodiment, there is a continuous, secure connection between the TTPR and the Attestation Client (89) throughout all steps (90c) through (92). In one embodiment, the Attestation Client (89) verifies the Attestor's identity and authority to attest before any steps (90c), (90e), or (91) are allowed to take place.

The system also encompasses a business process whereby some form of computer running or having access to an Attestation Client (89) is placed in various locations accessible to Pseudonym Owners. These "Attestation Stations" are staffed

with individuals who will serve as attestors. In one embodiment, the reliability of the attestors has been pre-screened. In one embodiment, unique physical tokens, such as smart cards, are available for sale at the Attestation Station locations to be used by Pseudonym Owners as a method of proving their ownership of a pseudonym. In one embodiment, devices for measuring Category 1 characteristics are available at the Attestation Stations. For example, such devices may be connected to the computer and may be used to directly transmit Category 1 characteristics into the computer. The Attestation Station may also be used to establish the authority to pick-up a package at a location, or to order a medical test under a pseudonym.

When a user wants to set up a new pseudonym, he or she contacts the TTPR and, after verifying his True Name or an existing pseudonym that is registered with the TTPR, requests the new pseudonym. If it is available, the pseudonym is registered with the TTPR and a certificate of ownership issues to the requester. In one embodiment, the standards for future identity verification are also established at the time the pseudonym is issued.

Pseudonym Structure

Part of a pseudonym may be the PseudoID, a unique identifier, preferably a large integer, that distinguishes the pseudonym from others. The PseudoID may be, without limitation, any one or more of: a public key, a sequentially, pseudo-randomly, or truly-randomly generated number, a unique mail, email, or domain address, a number imbedded in a token, a credit, debit, or financial institution account number, a number generated from biometric or other input, or a number generated by a government or other agency or organization for some other purpose. It is, of course, understood that any references to numbers herein encompasses strings, which may be represented as numbers. PseudoIDs may be generated by the Pseudonym Client, by the Pseudonym Server, or by a third party.

PseudoIDs may contain information in addition to a unique identifier, such as parity information to allow rapid checking of the validity of the PseudoID, some information about the issuer of the PseudoID, or imbedded credentials. In one embodiment, a PseudoID may optionally contain an "extension" code (a number appended to the PseudoID) which grants access to certain resources or information.

A pseudonym may have more parts than just a PseudoID, however. In the case where the PseudoID is associated with a token, the token itself may be considered to be an embodiment of a pseudonym. A pseudonym may also have a nym, domain name, email address, user ID for a computer system, user ID-password combination, or other user-comprehensible information associated with it. A nym itself may be formatted or otherwise mapped to have special applicability within one or more solution spaces, or may be used for convenience.

The system operates under the theory that all that most people need to get confidence sufficient for a significant interaction with a second person is assurance that someone they trust: (a) recognizes that second person and (b) is willing to attest to their knowledge of several characteristics of the second person. People gain confidence in others by accumulating many bits of information about them, and then by fitting that information into the patterns of their prior experiences. By allowing people to quickly and reliably gain information about the "faces" which individuals show in cyberspace, this system makes virtual social and economic interactions easier.

The present invention has been illustrated by description of a number of embodiments thereof. However, numerous modifications, which are contemplated as falling within the scope of the present invention, should now be apparent to those skilled in the art. Therefore, it is intended that the scope of the present invention be limited only by the scope of the properly construed claims appended hereto and equivalents thereof.

What is claimed is:

1. A system for verifying characteristics of an entity, the system comprising:

one or more modules programmed to:

accept proof of a right to use a pseudonym from an entity;

create one or more certificates which associates the pseudonym with one or more characteristics of the pseudonym or the entity without associating the pseudonym with the identity of the entity; and

send at least one of the one or more certificates to a recipient external to the system.

2. The system for verifying characteristics of an entity of claim 1, wherein at least one of the one or more modules are part of one or more computer systems.

3. The system for verifying characteristics of an entity of claim 1 or 2, wherein at least one of the one or more modules operates over the Internet.

4. The system for verifying characteristics of an entity of any of claims 1-3, wherein at least one of the one or more modules is located on a portable device.

5. The system for verifying characteristics of an entity of any of claims 1-4, wherein at least one of the one or more characteristics includes a characteristic verifiable by one of the following methods: through physical examination, through prolonged interaction, or by a third party.

6. The system for verifying characteristics of an entity of any of claims 1-5, wherein at least one of the one or more modules is further programmed to receive characteristic information from an external data source.

7. The system for verifying characteristics of an entity of any of claims 1-6, wherein at least one of the one or more certificates is a digital certificate.

8. The system for verifying characteristics of an entity of any of claims 1-7, wherein at least one of the one or more modules is further programmed to associate a characteristic associated with a first pseudonym with a second pseudonym.

9. The system for verifying characteristics of an entity of any of claims 1-8, wherein at least one of the one or more certificates includes one or more credentials.

10. The system for verifying characteristics of an entity of claim 9, wherein at least one of the one or more credentials included in the one or more certificates is directly or indirectly attributed to the pseudonym.

11. The system for verifying characteristics of an entity of claim 10, wherein the indirectly attributing of one or more characteristics to the pseudonym is accomplished by combining one or more characteristics of the pseudonym or cross-attributing one or more characteristics from other pseudonyms which the same entity has the right to use.

12. The system for verifying characteristics of an entity of claim 10, wherein the direct attributing is accomplished by an attestation.

13. The system for verifying characteristics of an entity of claim 12, wherein the attestation is given a reliability weight based on the reliability of an entity providing the attestation.

14. The system for verifying characteristics of an entity of claim 12, wherein an attestation collection process involves the transfer of an electronic form.

15. The system for verifying characteristics of an entity of any of claims 9-14, wherein at least one of the one or more certificates includes information about the reliability of the source or sources of information contained in the one or more credentials.

16. The system for verifying characteristics of an entity of any of claims 1-15, wherein at least one of the one or more modules is further programmed to detect a reference loop.

17. The system for verifying characteristics of an entity of any of claims 1-16, wherein at least one of the one or more certificates includes information about when the entity proved its right to use the pseudonym.

18. The system for verifying characteristics of an entity of any of claims 1-17, wherein at least one of the one or more certificates expires within a limited time.

19. The system for verifying characteristics of an entity of any of claims 1-18, wherein at least one of the one or more modules further programmed to screen outgoing messages to prevent undesired identity or characteristic information from being sent.

20. The system for verifying characteristics of an entity of any of claims 1-19, wherein at least one of the one or more modules maintains a voice connection and wherein at least one of the one or more characteristics is a characteristic of an entity at one end of the voice connection.

21. The system for verifying characteristics of an entity of any of claims 1-20, wherein at least one of the one or more certificates contains information certifying the right of the entity to gain access to a restricted group or location.

22. The system for verifying characteristics of an entity of any of claims 1-21, wherein at least one of the one or more certificates contains a ballot and information certifying the right of the entity to vote.

23. The system for verifying characteristics of an entity of any of claims 1-22, wherein at least one of the one or more certificates contains information certifying the right of the entity to send messages to a particular recipient.

24. The system for verifying characteristics of an entity of any of claims 1-23, wherein at least one of the one or more certificates contains information certifying the right of the entity to access restricted data or services.

25. The system for verifying characteristics of an entity of any of claims 1-24, wherein at least one of the one or more certificates contains financial information certifying the right or ability of the entity to engage in one of the following: a financial transaction, an insurance transaction, a medical transaction, an employment transaction, or a consumer transaction.

26. The system for verifying characteristics of an entity of any of claims 1-25, wherein at least one of the one or more modules is further programmed to send location and movement information of the entity to an authorized entity.

27. The system for verifying characteristics of an entity of any of claims 1-26, wherein accepting proof of the right to use a pseudonym involves taking a biometric measurement.

28. The system for verifying characteristics of an entity of any of claims 1-27, wherein accepting proof of the right to use a pseudonym receiving a key obtainable from a third party.

29. The system for verifying characteristics of an entity of any of claims 1-28, wherein accepting proof of the right to use a pseudonym checking an electrical token.

30. The system for verifying characteristics of an entity of any of claims 1-29, wherein the recipient is the entity.

31. The system for verifying characteristics of an entity of any of claims 1-30, wherein the recipient is a client computer.

32. The system for verifying characteristics of an entity of any of claims 1-31, wherein the proof of the right to use a pseudonym involves a key obtainable from a third party.

33. The system for verifying characteristics of an entity of any of claims 1-32, wherein the proof of the right to use a pseudonym involves an electrical token.

34. The system for verifying characteristics of an entity of any of claims 1-33, wherein the system includes a client computer executing one of the modules which includes instructions to:

send and receive proof of a right to use a pseudonym from an entity;

send and receive one or more certificates which associate the pseudonym with one or more characteristics of the pseudonym or the entity without associating the pseudonym with the identity of the entity.

35. The system for verifying characteristics of an entity of claim 34, wherein the client computer further includes instructions to screen outgoing messages to prevent undesired identity or characteristic information from being sent.

36. The system for verifying characteristics of an entity of any of claims 1-35, wherein the system includes a server executing one of the modules which includes instructions to:

send and receive proof of a right to use a pseudonym;

create one or more certificates which associates a pseudonym with one or more characteristics of the pseudonym or entity without associating the pseudonym with the identity of the entity; and

send at least one of the one or more certificates to a recipient external to the system.

37. The system for verifying characteristics of an entity of claim 36, wherein the server further includes instructions to store pseudonym characteristic information.

38. A method for verifying characteristics of an entity, the method comprising:

accepting proof of a right to use a pseudonym from an entity;

creating one or more certificates which associates the pseudonym with one or more characteristics of the pseudonym of the entity without associating the pseudonym with the identity of the entity; and

sending at least one of the one or more certificates to a recipient external to the system.

39. The method for verifying characteristics of an entity of claim 38, wherein the recipient is the entity.

40. The method for verifying characteristics of an entity of claim 38 or 39, wherein the recipient is a client computer.

41. The method for verifying characteristics of an entity of any of claims 38-40, wherein part of the method is executed on one or more computer systems.

42. The method for verifying characteristics of an entity of any of claims 38-41, further comprising connecting to the Internet.

43. The method for verifying characteristics of an entity of any of claims 38-42, wherein part of the method is executed on a portable device.

44. The method for verifying characteristics of an entity of any of claims 38-43, wherein at least one of the one or more characteristics includes a characteristic verifiable by one of the following methods: through physical examination, through prolonged interaction, or by a third party.

45. The method for verifying characteristics of an entity of any of claims 38-44, further comprising receiving characteristic information from an external data source.

46. The method for verifying characteristics of an entity of any of claims 38-45, wherein at least one of the one or more certificates is a digital certificate.

47. The method for verifying characteristics of an entity of any of claims 38-46, further comprising associating a characteristic associated with a first pseudonym with a second pseudonym.

48. The method for verifying characteristics of an entity of any of claims 38-47, wherein at least one of the one or more certificates includes one or more credentials.

49. The method for verifying characteristics of an entity of claim 48, further comprising directly or indirectly attributing to the pseudonym at least one of the one or more credentials included in the one or more certificates.

50. The method for verifying characteristics of an entity of claim 49, wherein the indirectly attributing of one or more characteristics to the pseudonym is accomplished by combining one or more characteristics of the pseudonym or cross-attributing one or more characteristics from other pseudonyms which the same entity has the right to use.

51. The method for verifying characteristics of an entity of claim 49, wherein the direct attributing is accomplished by an attestation.

52. The method for verifying characteristics of an entity of claim 51, further comprising giving a reliability weight to the attestation based on the reliability of an entity providing the attestation.

53. The method for verifying characteristics of an entity of claim 51, further comprising attestation collection process which involves the transfer of an electronic form.

54. The method for verifying characteristics of an entity of any of claims 48-53, wherein at least one of the one or more certificates includes information about the reliability of the source or sources of information contained in the one or more credentials.

55. The method for verifying characteristics of an entity of any of claims 38-54, further comprising detecting a reference loop.

56. The method for verifying characteristics of an entity of any of claims 38-55, wherein at least one of the one or more certificates includes information about when the entity proved its right to use the pseudonym.

57. The method for verifying characteristics of an entity of any of claims 38-56, wherein at least one of the one or more certificates expires within a limited time.

58. The method for verifying characteristics of an entity of any of claims 38-57, further comprising screening outgoing messages to prevent undesired identity or characteristic information from being sent.

59. The method for verifying characteristics of an entity of any of claims 38-58, further comprising maintaining a voice connection and wherein at least one of the one or more characteristics is a characteristic of an entity at one end of the voice connection.

60. The method for verifying characteristics of an entity of any of claims 38-59, wherein at least one of the one or more certificates contains information certifying the right of the entity to gain access to a restricted group or location.

61. The method for verifying characteristics of an entity of any of claims 38-60, wherein at least one of the one or more certificates contains a ballot and information certifying the right of the entity to vote.

62. The method for verifying characteristics of an entity of any of claims 38-61, wherein at least one of the one or more certificates contains information certifying the right of the entity to send messages to a particular recipient.

63. The method for verifying characteristics of an entity of any of claims 38-62, wherein at least one of the one or more certificates contains information certifying the right of the entity to access restricted data or services.

64. The system for verifying characteristics of an entity of any of claims 38-63, wherein at least one of the one or more certificates contains financial information certifying the right or ability of the entity to engage in one of the following: a financial transaction, an insurance transaction, a medical transaction, an employment transaction, or a consumer transaction.

65. The method for verifying characteristics of an entity of any of claims 38-64, further comprising sending location and movement information of the entity to an authorized entity.

66. The method for verifying characteristics of an entity any of claims 38-65, wherein accepting proof of the right to use a pseudonym involves taking a biometric measurement.

67. The method for verifying characteristics of an entity any of claims 38-66, wherein accepting proof of the right to use a pseudonym involves receiving a key obtainable from a third party.

68. The method for verifying characteristics of an entity any of claims 38-67, wherein accepting proof of the right to use a pseudonym involves checking an electrical token.

69. The method for verifying characteristics of an entity of any of claims 38-68, wherein a reliability of an attestor is calculated by:

for each of a characteristic attestation made:

for each on of one or more pseudonym for which the character attestation was made:

for each time another entity attested to that characteristic:

verify or contradict the attestation;

if the attestation is verified, add one to a verification counter (v);

if the attestation is contradicted, add one to a contradiction counter (c);

if there are no contradictions, add one to the attestation counter (A);

if there are contradictions, calculate the raw reliability weight (R_{ACP}) for the attestor for a characteristic of a pseudonym as:

$R_{ACP} = v/(v + m*C)$ where m is a reliability coefficient;

calculate the raw reliability weight for attestor for a characteristic R_{ACP} as the average of all values of R_{AC} for all pseudonyms; and

calculate the raw reliability weight (R_A)as the average (R_{AC}) of for all characteristics.

70. A computer readable medium on which is encoded a software program including computer instructions which when executed by a computer cause the computer to execute a sequence of steps comprising:

accepting proof of a right to use a pseudonym from an entity;

creating one or more certificates which associates the pseudonym with one or more characteristics of the pseudonym of the entity without associating the pseudonym with the identity of the entity; and

sending at least one of the one or more certificates to a recipient external to the system.

71. The computer readable medium of claim 70, the sequence of steps further comprising connecting to the Internet.

72. The computer readable medium of claim 70 or 71, wherein the computer readable medium is located on a portable device.

73. The computer readable medium of any of claims 70-72, wherein at least one of the one or more characteristics includes a characteristic verifiable through physical examination.

74. The computer readable medium of any of claims 70-73, wherein at least one of the one or more characteristics includes a characteristic verifiable through prolonged interaction.

75. The computer readable medium of any of claims 70-74, wherein at least one of the one or more characteristics includes a characteristic verifiable by a third party.

76. The computer readable medium of any of claims 70-75, receiving characteristic information from an external data source.

77. The computer readable medium of any of claims 70-76, wherein at least one of the one or more certificates is a digital certificate.

78. The computer readable medium of any of claims 70-77, associating a characteristic associated with a first pseudonym with a second pseudonym.

79. The computer readable medium of any of claims 70-78, wherein at least one of the one or more certificates includes one or more credentials.

80. The computer readable medium of claim 79, directly or indirectly attributing to the pseudonym at least one of the one or more credentials included in the one or more certificates.

81. The computer readable medium of claim 80, wherein the indirectly attributing of one or more characteristics to the pseudonym is accomplished by combining one or more

characteristics of the pseudonym or cross-attributing one or more characteristics from other pseudonyms which the same entity has the right to use.

82. The computer readable medium of claim 80, wherein the direct attributing is accomplished by an attestation.

83. The computer readable medium of claim 82, the sequence of steps further comprising giving a reliability weight to the attestation based on the reliability of an entity providing the attestation.

84. The computer readable medium of claim 82, the sequence of steps further comprising an attestation collection process involving the transfer of an electronic form.

85. The computer readable medium of claims 79-84, wherein at least one of the one or more certificates includes information about the reliability of the source or sources of information contained in the one or more credentials.

86. The computer readable medium of any of claims 70-85, the sequence of steps further comprising detecting a reference loop.

87. The computer readable medium of any of claims 70-86, wherein at least one of the one or more certificates includes information about when the entity proved its right to use the pseudonym.

88. The computer readable medium of any of claims 70-87, wherein at least one of the one or more certificates expires within a limited time.

89. The computer readable medium of any of claims 70-88, the sequence of steps further comprising screening outgoing messages to prevent undesired identity or characteristic information from being sent.

90. The computer readable medium of any of claims 70-89, the sequence of steps further comprising maintaining a voice connection and wherein at least one of the one or more characteristics is a characteristic of an entity at one end of the voice connection.

91. The computer readable medium of any of claims 70-90, wherein at least one of the one or more certificates contains information certifying the right of the entity to gain access to a restricted group or location.

92. The computer readable medium of any of claims 70-91, wherein at least one of the one or more certificates contains a ballot and information certifying the right of the entity to vote.

93. The computer readable medium of any of claims 70-92 wherein at least one of the one or more certificates contains information certifying the right of the entity to send messages to a particular recipient.

94. The computer readable medium of any of claims 70-93, wherein at least one of the one or more certificates contains information certifying the right of the entity to access restricted data or services.

95. The computer readable medium of any of claims 70-94, wherein at least one of the one or more certificates contains financial information certifying the right or ability of the entity to engage in a financial transaction.

96. The computer readable medium of any of claims 70-95, wherein at least one of the one or more certificates contains insurance information certifying the right or ability of the entity to engage in an insurance transaction.

97. The computer readable medium of any of claims 70-96, wherein at least one of the one or more certificates contains medical information certifying the right or ability of the entity to engage in a medical transaction.

98. The computer readable medium of any of claims 70-97, wherein at least one of the one or more certificates contains employment information certifying the right or ability of the entity to engage in an employment transaction.

99. The computer readable medium of any of claims 70-98, wherein at least one of the one or more certificates contains consumer information certifying the right or ability of the entity to engage in a consumer transaction.

100. The computer readable medium of any of claims 70-99, the sequence of steps further comprising sending location and movement information of the entity to an authorized entity.

101. The computer readable medium of any of claims 70-100, wherein the step of accepting proof of a right to use a pseudonym involves taking a biometric measurement.

102. The computer readable medium of any of claims 70-101, wherein the step of accepting proof of a right to use a pseudonym involves receiving a key obtainable from a third party.

103. The computer readable medium of any of claims 70-102, wherein the step of accepting proof of a right to use a pseudonym involves checking an electrical token.

Figure 1

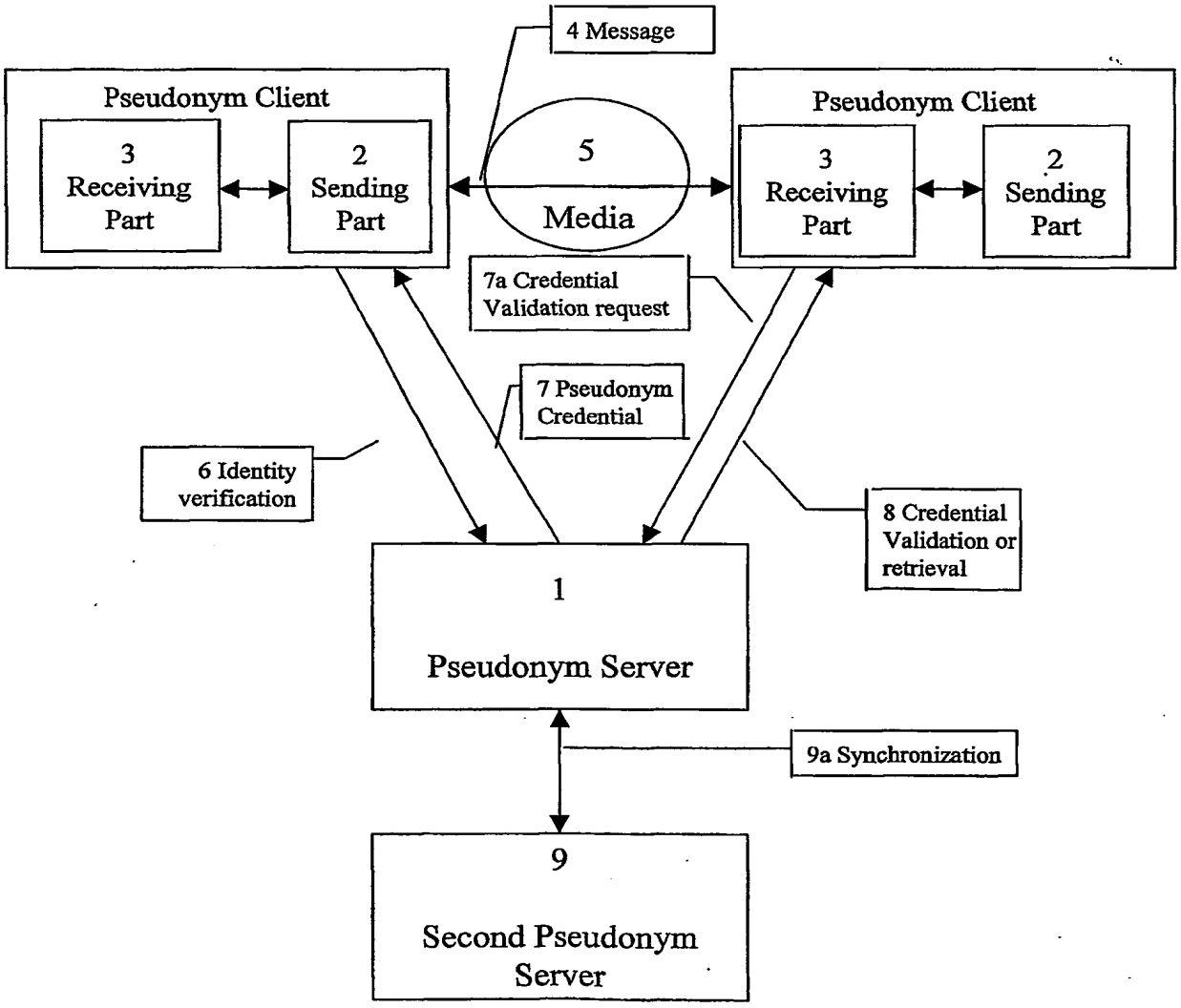

4 Message
Pseudonym Client
3 Receiving Part
2 Sending Part
5 Media
Pseudonym Client
3 Receiving Part
2 Sending Part
7a Credential Validation request
7 Pseudonym Credential
6 Identity verification
8 Credential Validation or retrieval
1 Pseudonym Server
9a Synchronization
9 Second Pseudonym Server

Figure 2

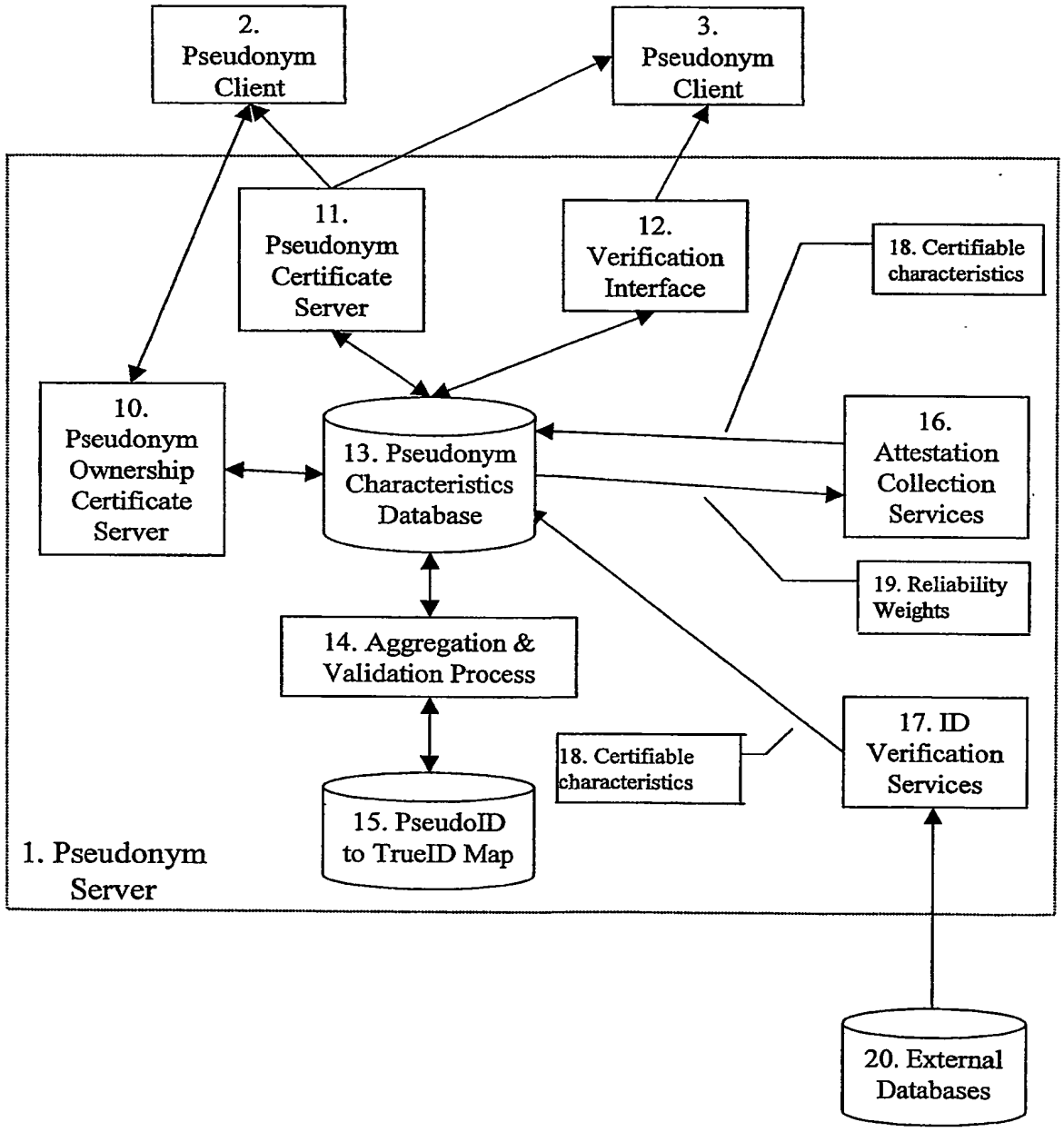

2. Pseudonym Client
3. Pseudonym Client
11. Pseudonym Certificate Server
12. Verification Interface
18. Certifiable characteristics
10. Pseudonym Ownership Certificate Server
13. Pseudonym Characteristics Database
16. Attestation Collection Services
19. Reliability Weights
14. Aggregation & Validation Process
17. ID Verification Services
18. Certifiable characteristics
15. PseudoID to TrueID Map
1. Pseudonym Server
20. External Databases

Figure 3

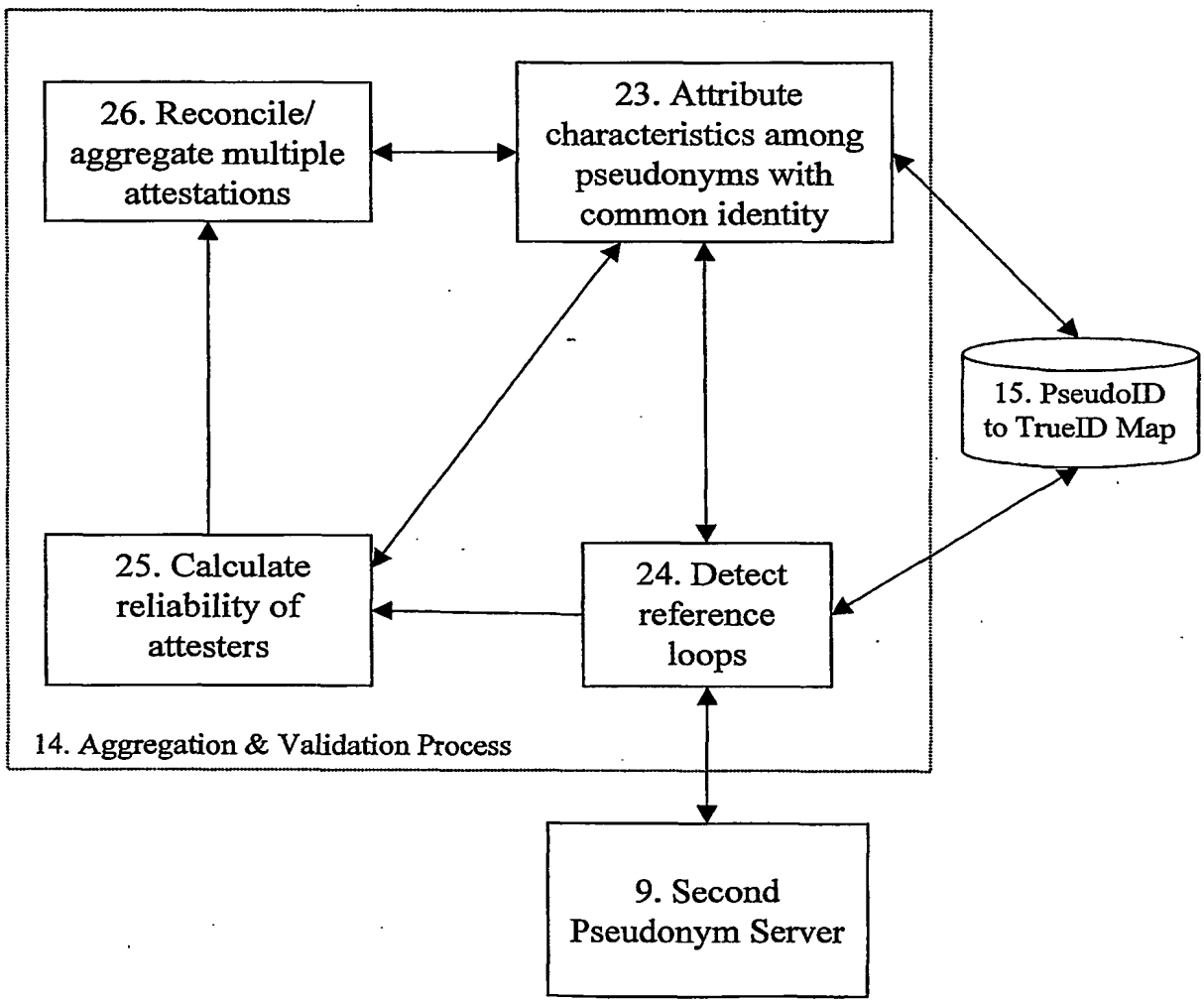

26. Reconcile/ aggregate multiple attestations
23. Attribute characteristics among pseudonyms with common identity
15. PseudoID to TrueID Map
25. Calculate reliability of attesters
24. Detect reference loops
14. Aggregation & Validation Process
9. Second Pseudonym Server

Figure 4

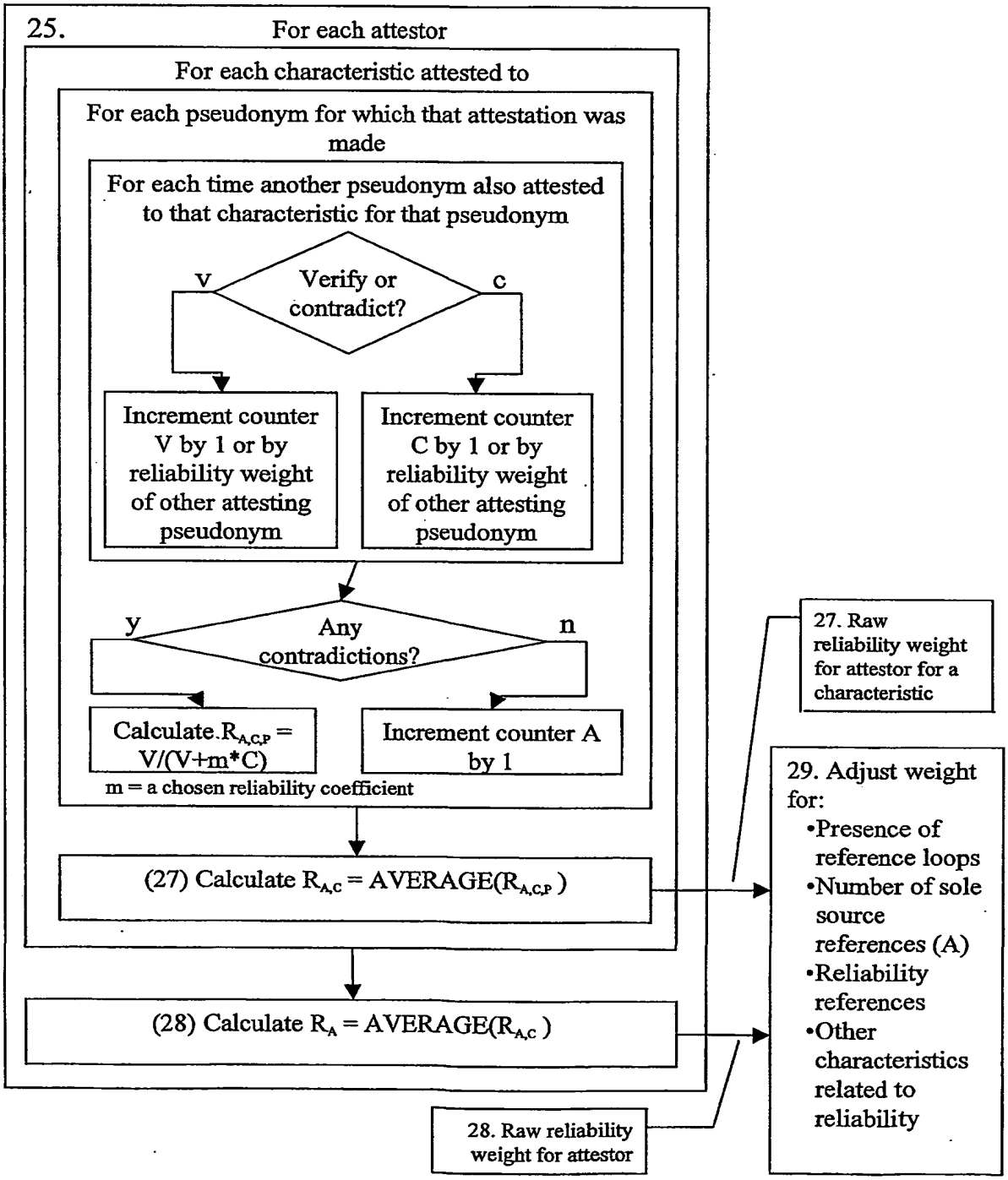

25.
For each attestor
For each characteristic attested to
For each pseudonym for which that attestation was made
For each time another pseudonym also attested to that characteristic for that pseudonym
Verify or contradict?
v
c
Increment counter V by 1 or by reliability weight of other attesting pseudonym
Increment counter C by 1 or by reliability weight of other attesting pseudonym
Any contradictions?
y
n
Calculate $R_{A,C,P}$ = V/(V+m*C)
Increment counter A by 1
m = a chosen reliability coefficient
(27) Calculate $R_{A,C}$ = AVERAGE($R_{A,C,P}$)
(28) Calculate R_A = AVERAGE($R_{A,C}$)
27. Raw reliability weight for attestor for a characteristic
28. Raw reliability weight for attestor
29. Adjust weight for:
•Presence of reference loops
•Number of sole source references (A)
•Reliability references
•Other characteristics related to reliability

Figure 5

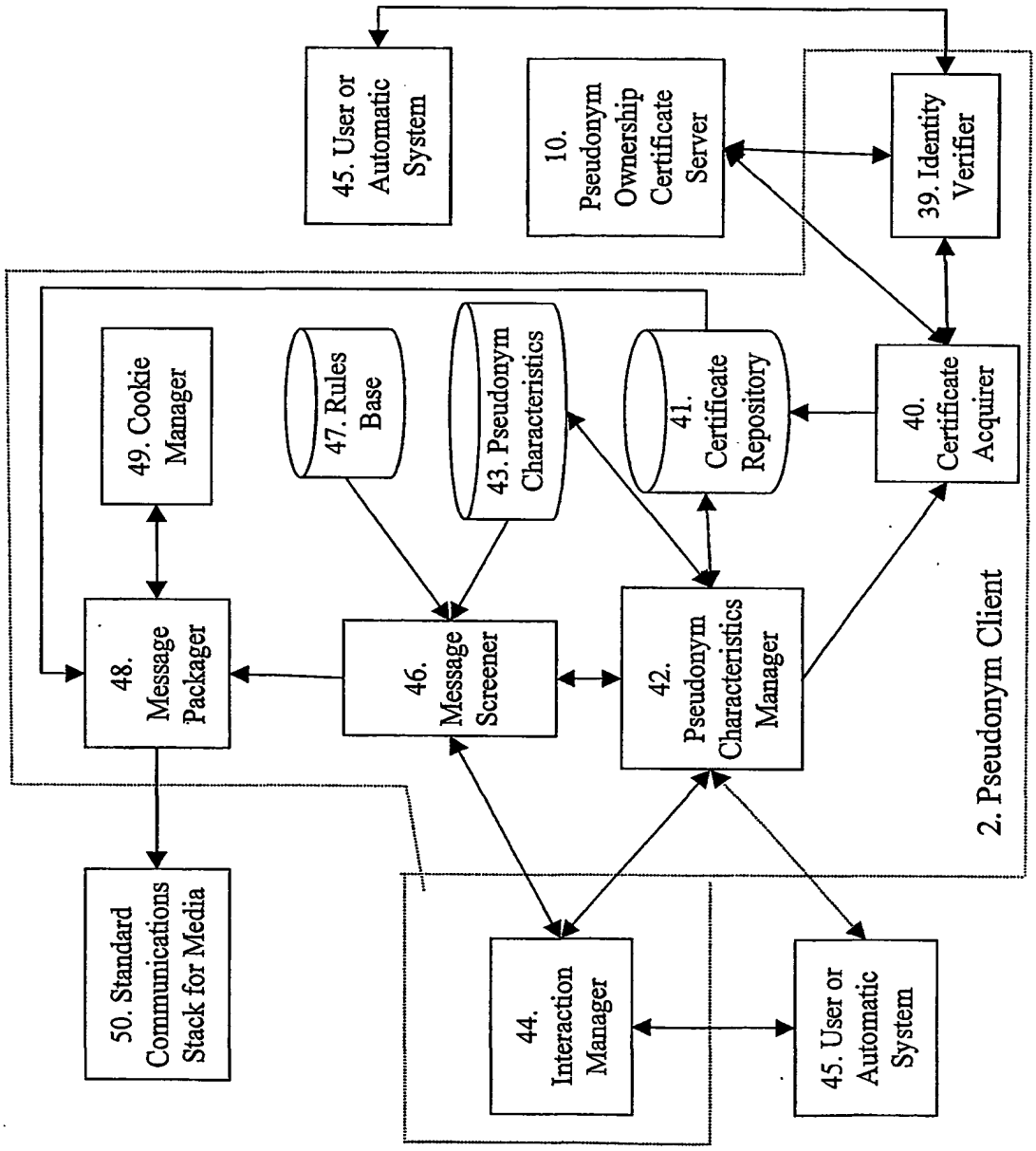

45. User or Automatic System
10. Pseudonym Ownership Certificate Server
39. Identity Verifier
49. Cookie Manager
47. Rules Base
43. Pseudonym Characteristics
41. Certificate Repository
40. Certificate Acquirer
48. Message Packager
46. Message Screener
42. Pseudonym Characteristics Manager
2. Pseudonym Client
50. Standard Communications Stack for Media
44. Interaction Manager
45. User or Automatic System

Figure 6

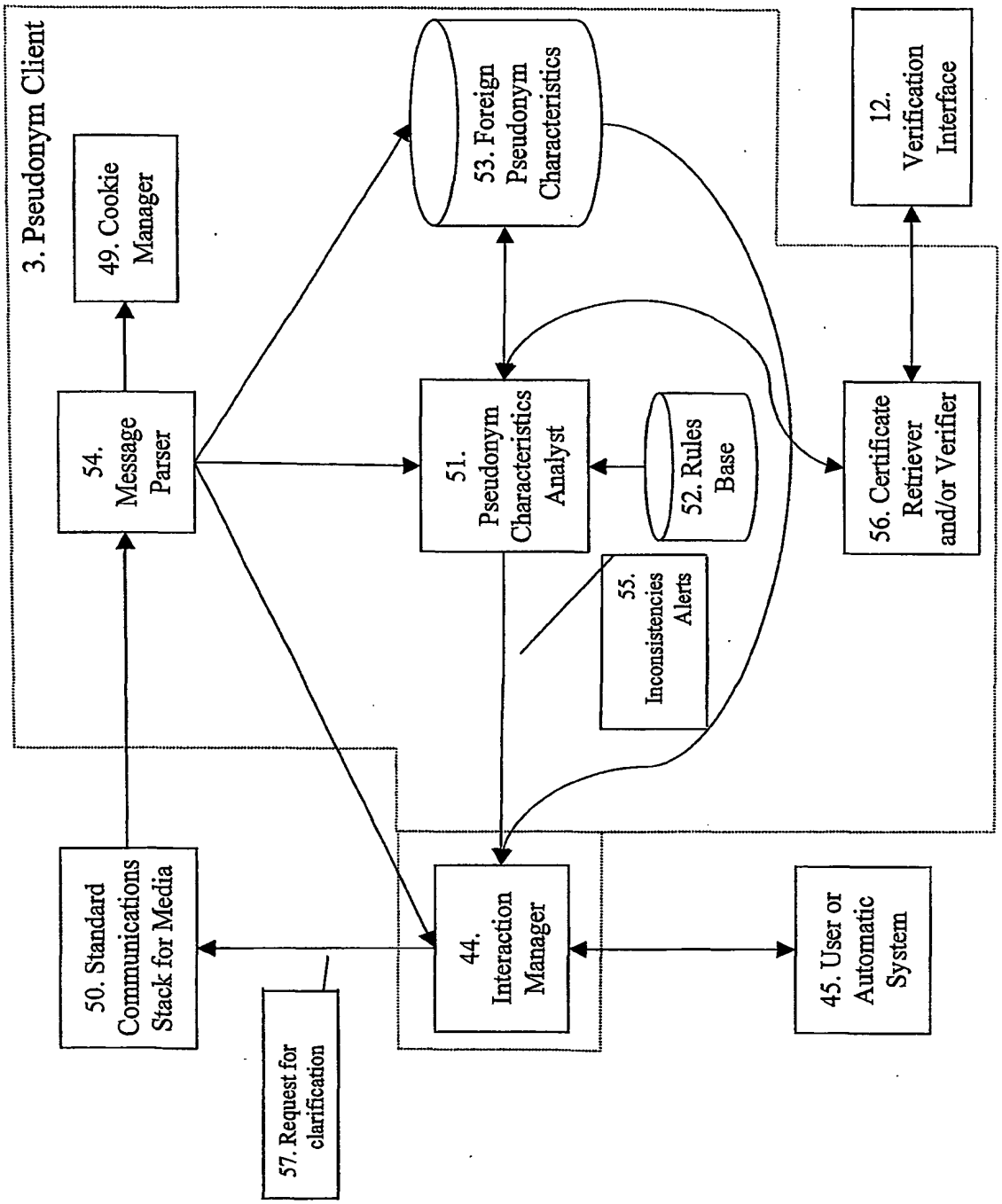

3. Pseudonym Client
49. Cookie Manager
53. Foreign Pseudonym Characteristics
12. Verification Interface
54. Message Parser
51. Pseudonym Characteristics Analyst
52. Rules Base
56. Certificate Retriever and/or Verifier
55. Inconsistencies Alerts
50. Standard Communications Stack for Media
44. Interaction Manager
45. User or Automatic System
57. Request for clarification

Figure 7

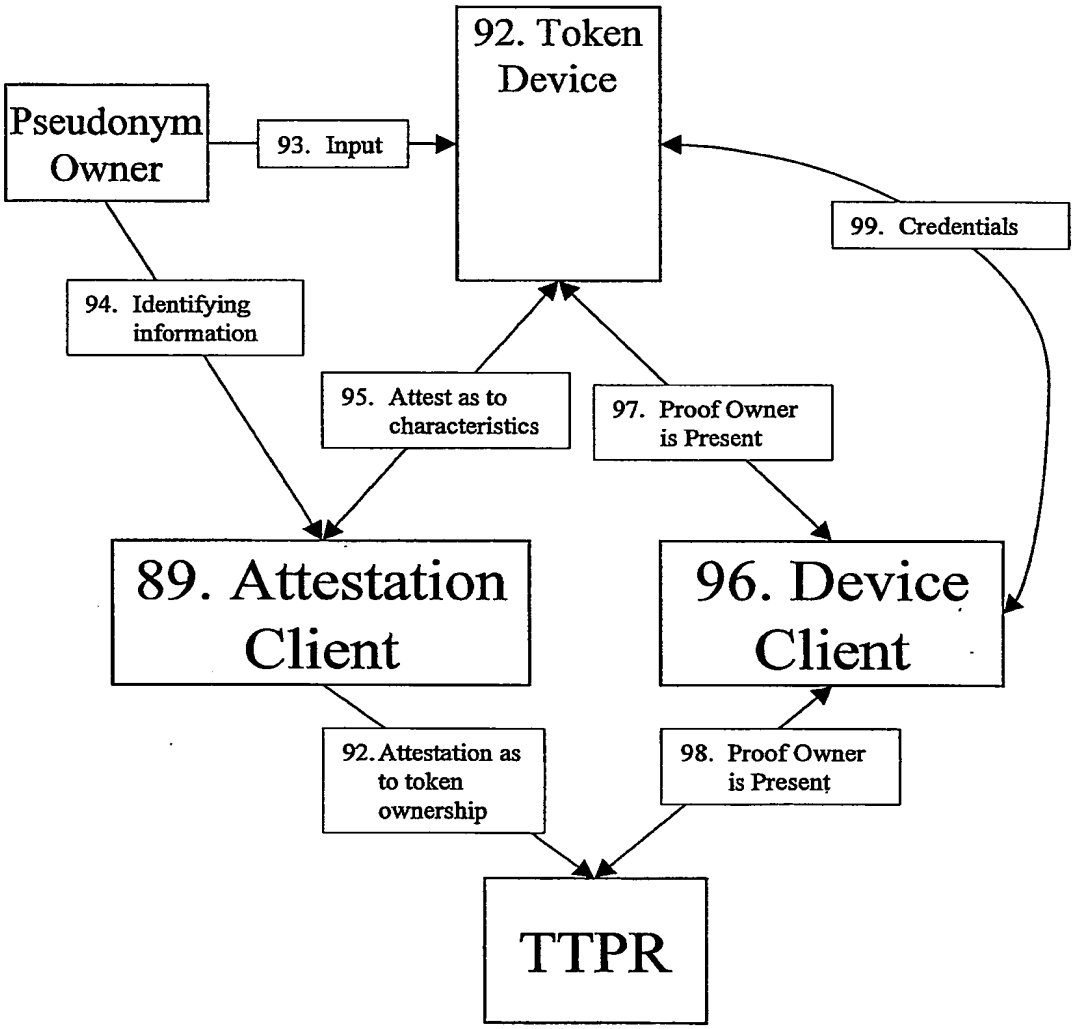

92. Token Device
Pseudonym Owner
93. Input
99. Credentials
94. Identifying information
95. Attest as to characteristics
97. Proof Owner is Present
89. Attestation Client
96. Device Client
92. Attestation as to token ownership
98. Proof Owner is Present
TTPR

Figure 8 Attestation Client